CLAIMS:

1. A method for authenticating a message, comprising:

performing a security function upon the message;

sending the message to a receiver;

sending the output of the security function to a target;

sending at least one publicly known constant to the receiver;

authenticating the received message as a function of at least a shared key, the received publicly known constants, the security function, the received message, and the output of the security function.

2. The method of Claim 1, wherein the security function comprises a hash function.

3. The method of Claim 1, wherein the authentication comprises a determination that the message is authentic.

4. The method of Claim 1, wherein the authentication comprises a determination that the message is not authentic.

5. The method of Claim 1, wherein the security function further comprises an encryption function.

6. The method of Claim 1, wherein the security function further comprises a decryption function.

7. A system for authenticating messages, comprising:

a source node having a shared key, security logic and publicly known constants; and

a target node also having the shared key and the security logic, the target node further configured to receive publicly known constants from the source node.

8. The system of Claim 7, wherein the source node comprises a computer.

9. The system of Claim 7, wherein the security logic is configured to implement a hashing function.

10. The system of Claim 7, further comprising an unsecured medium coupled between an output of the source node and an input of the target node.

11. The system of Claim 7, wherein the source node is further configured to generate a message authentication code (MAC).

12. The system of Claim 7, wherein the MAC is a function of at least a message, the secret key, the security function and the publicly known constants.

13. The system of Claim 7, wherein the target node is further configured to receive a message authentication code (MAC).

14. The system of Claim 13, wherein the target node is further configured to employ the MAC to authenticate a received message from the source node.

15. A computer program product for authenticating a message, the computer program product having a medium with a

computer program embodied thereon, the computer program comprising:

computer code for performing a security function upon the message;

computer code for sending the message to a target;

computer code for sending the output of the security function to the target;

computer code for sending at least one publicly known constant to the target; and

computer code for authenticating the received message as a function of at least a shared key, the received publicly known constants, the security function, and the received message.

16. A processor for authenticating a message, the processor including a computer program comprising:

computer code for performing a security function upon the message;

computer code for sending the message to a target;

computer code for sending the output of the security function to the target;

computer code for sending at least one publicly known constant to the target; and

computer code for authenticating the received message as a function of at least a shared key, the received publicly known constants, the security function, and the received message.